

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-001090

(43)Date of publication of application : 05.01.1990

(51)Int.Cl. G06K 19/073
G06F 12/14
G06K 17/00

(21)Application number : 01-002899 (71)Applicant : HITACHI MAXELL LTD

(22)Date of filing : 11.01.1989 (72)Inventor : SHINAGAWA TORU

(30)Priority

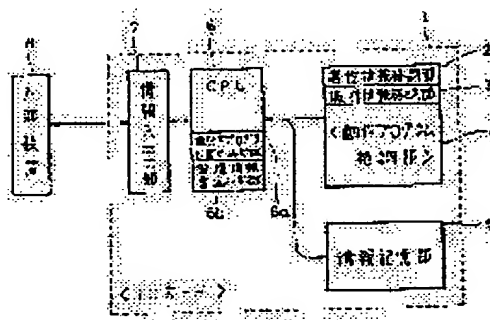
Priority number : 63 21919 Priority date : 03.02.1988 Priority country : JP

(54) IC CARD AND METHOD FOR WRITING ITS OPERATION PROGRAM

(57)Abstract:

PURPOSE: To improve an operation program and the confidentiality of the rewriting of the program and to prevent the illegal rewriting of the program by controlling the possibility of the rewriting of the program in an IC card and giving authority to rewrite the program according to the coincidence of collated information.

CONSTITUTION: When the operation program is to be written or rewritten, an instruction from an external device 8 is decoded in a CPU6, and when the decoded instruction is the one for the writing of an operating processor, an operation program writing control program 6a in the CPU6 is started and executed. On the other hand, when identification information is already written, the identification information is read from an identification information storing part 3, and the collation between the read identification information and input identification information is executed. Further, it is decided whether both the pieces of identification information coincide with each other or not, and the input new identification information or attribute information is accepted only when both the pieces of identification information coincide with each other. The CPU6 decides whether both the pieces of identification information coincide or not, stores either the identification information or the attribute information to a corresponding storing part in either an attribute information storing part 2 or the identification information storing part 3, and executes rewriting processing for both pieces of information.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A) 平2-1090

⑬ Int.Cl.³

識別記号

庁内整理番号

⑭ 公開 平成2年(1990)1月5日

G 06 K 19/073

G 06 F 12/14

G 06 K 17/00

3 1 0

D

E

7737-5B

6711-5B

6711-5B

G 06 K 19/00

P

審査請求 未請求 請求項の数 12 (全16頁)

⑮ 発明の名称 ICカード及びその動作プログラム書込み方法

⑯ 特 願 平1-2899

⑰ 出 願 平1(1989)1月11日

優先権主張 ⑱ 昭63(1988)2月3日 ⑲ 日本(JP) ⑳ 特願 昭63-21919

㉑ 発 明 者 品 川 徹 大阪府茨木市丑寅1丁目1番88号 日立マクセル株式会社
内

㉒ 出 願 人 日立マクセル株式会社 大阪府茨木市丑寅1丁目1番88号

㉓ 代 理 人 弁理士 梶山 信是 外1名

明 細 書

1. 発明の名称

ICカード及びその動作プログラム書込み方法

2. 特許請求の範囲

(1) その内部に動作プログラムとこの動作プログラムに応じて所定の処理を実行するプロセッサとを有し、前記動作プログラムの書換えが可能なICカードにおいて、前記動作プログラムの書換えが可能な否かを示す書換え可否情報とこの書換え可否情報を書換え可及び書換え不可のいずれかの状態に書換える許可を与えるための照合情報とを記憶するメモリを備え、外部からの入力情報と前記照合情報との一致をもって前記書換え可否情報の状態を可及び否のいずれか一方の情報に書換え、この書換え可否情報が書換え可となっているときに前記動作プログラムの書換え処理を実行することを特徴とするICカード。

(2) 動作プログラムを記憶したメモリとこの動作プログラムに応じて所定の処理を実行するプロセッサとを有し、前記動作プログラムの書換えが可

能なICカードにおいて、前記動作プログラムの書換えが可能な否かを示す書換え可否情報とこの書換え可否情報を書換え可及び書換え不可のいずれかの状態に書換える許可を与えるための照合情報とを記憶する記憶領域を前記メモリ及び他のメモリのいずれかに設け、外部からの入力情報と前記記憶領域に記憶された前記照合情報との一致をもって前記書換え可否情報の状態を可及び否のいずれか一方の情報に書換え、この書換え可否情報が書換え可となっているときに前記動作プログラムの書換え処理を実行することを特徴とするICカード。

(3) 入力情報と照合情報との一致をもって書換え可否情報の状態を書換えるプログラムと、この書換え可否情報が書換え可となっているときに動作プログラムの書換え処理を行うプログラムとを有して、照合情報はカード取扱者を識別するための識別情報であることを特徴とする請求項1又は2記載のICカード。

(4) 動作プログラムを記憶したメモリは書換え可

能な不揮発性メモリであることを特徴とする請求項3記載のICカード。

(5) 照合情報は動作プログラムを識別する識別情報であることを特徴とする請求項1又は2記載のICカード。

(6) 照合情報はカード取扱者を識別する情報と動作プログラムを識別する識別情報とを有することを特徴とする請求項1又は2記載のICカード。

(7) その内部に複数の動作プログラムとこれらの動作プログラムの1つを起動し、この起動したプログラムに応じて所定の処理を実行するプロセッサとを有し、前記動作プログラムの書換えが可能なICカードにおいて、前記複数の動作プログラムのそれぞれに対応して動作プログラムの書換えが可能か否かを示す書換え可否情報とこの書換え可否情報を書換え可及び書換え不可のいずれかの状態に書換える許可を与えるための照合情報とをそれぞれ記憶する記憶領域を前記メモリ及び他のメモリのいずれかに設け、前記複数の動作プログラムのうちから選択された動作プログラムに対応

する外部から入力された入力情報と前記記憶領域に記憶された前記照合情報との一致をもって前記選択された動作プログラムについての前記書換え可否情報の状態を可及び否のいずれか一方の情報に書換え、この書換え可否情報が書換え可となっているときに前記選択された動作プログラムの書換え処理を実行することを特徴とするICカード。

(8) 記憶領域は動作プログラムを記憶しないメモリに設けられることを特徴とする請求項7又は8記載のICカード。

(9) 記憶領域は複数の動作プログラムのそれぞれに対応して設けられていることを特徴とする請求項7記載のICカード。

(10) 動作プログラムはシステムプログラムを含むことを特徴とする請求項7記載のICカード。

(11) 動作プログラムを格納するための動作プログラム記憶領域と前記動作プログラム記憶領域に動作プログラムの書込みが可能か否かを示す書換え可否情報を格納する属性情報記憶領域とこの属性情報記憶領域に記憶された書換え可否情報を書換

え可及び不可のいずれか一方の情報に書換える許可を与えるための識別情報が記憶される識別情報記憶領域とを有するメモリと、外部からの入力情報と前記識別情報記憶領域に記憶された識別情報との一致をもって前記識別情報を前記属性情報記憶領域に記憶する識別情報書込み手段と、前記属性情報記憶領域に記憶されている識別情報が書換え可となっているときに外部から提供される動作プログラムを前記動作プログラム記憶領域に記憶する動作プログラム書込み手段と、前記動作プログラムに応じてその処理を実行する実行処理部とを備え、前記識別情報書込み手段により前記属性情報記憶領域に書換え可を示す識別情報を記憶した後、前記動作プログラム書込み手段により外部から提供される動作プログラムを前記動作プログラム記憶領域に記憶し、前記識別情報書込み手段により前記属性情報記憶領域に書換え不可を示す識別情報を記憶することを特徴とするICカードの動作プログラム書込み方法。

(12) 動作プログラムを格納するための動作プロ

グラム記憶領域と前記動作プログラム記憶領域に動作プログラムの書込みが可能か否かを示す識別情報を格納する属性情報記憶領域とこの属性情報記憶領域に記憶された識別情報を書換え可及び不可のいずれか一方の情報に書換える許可を与えるための識別情報が記憶される識別情報記憶領域とを有するメモリと、外部からの入力情報と前記識別情報記憶領域に記憶された識別情報との一致をもって前記識別情報を前記属性情報記憶領域に記憶する識別情報書込み手段と、前記属性情報記憶領域に記憶されている識別情報が書換え可となっているときに外部から提供される動作プログラムを前記動作プログラム記憶領域に記憶する動作プログラム書込み手段と、前記動作プログラムに応じてその処理を実行する実行処理部とを備え、前記識別情報書込み手段により前記属性情報記憶領域に書換え可を示す識別情報を記憶した後、前記動作プログラム書込み手段により外部から提供されるICカードの動作をテストするためのテストプログラムを前記動作プログラム記憶領域に記憶

し、動作テストが終了後に正しい動作をしたICカードについて前記動作プログラム書込み手段により外部から提供される動作プログラムを前記動作プログラム記憶領域に記憶し、前記識別情報書込み手段により前記属性情報記憶領域に書換え不可を示す識別情報を記憶することを特徴とするICカードの動作プログラム書込み方法。

3. 発明の詳細な説明

〔産業上の利用分野〕

この発明はICカード及びその動作プログラム書込み方法に関し、詳しくは、その動作プログラムの書換えが権限のあるもの以外できないようなICカードとその動作プログラム書込み方法に関する。

〔従来の技術〕

商品取引でのクレジットシステムとか、現金の受け渡しを行う銀行の支払/預金システム、病院とか社員食堂等における各種の精算システムなどがICカードを用いるシステムとして実用化されているが、このようなICカードによるシステム

では、その不正使用が大きな問題となる。

ICカードは、通常、内部にマイクロプロセッサとメモリ、そして外部装置との間でデータの授受を行うためのインタフェース等とを内蔵している、例えば、外部装置の一つであるホストコンピュータとか、ICカードリーダー・ライタに装着されて使用される。そして、外部装置から発信されたコマンド群をICカードの内部制御プログラムが解釈し、メモリに記憶された動作プログラムに従って、そのメモリのアクセス、例えばデータの書込み、読出し及び消去等を実行し、その結果をコマンドのレスポンスとして外部装置に返答するシーケンスに従って外部装置との間でデータの授受を行う。

ICカードに格納されるプログラムには、内蔵されるマイクロプロセッサ自体の制御動作に関するプログラムとか、基本的な内部回路等の制御のプログラムのほかに、マイクロプロセッサに対して特定の機能に応じて特定の処理を実行させる動作プログラム(テストプログラムとか、各種のA

プリケーションプログラム等を含む)とがある。

一般に、前者のプログラムの多くは、マイクロプロセッサとともに作られ、マスクROM等の中に格納されているので容易に書換えることはできないが、後者の動作プログラムは、後からホストコンピュータ等からメモリにダウンロードされる関係で、その書換えが可能である。

〔解決しようとする課題〕

ダウンロードでプログラムを後から書込むICカードとしては、例えば、特開昭81-211788号公報に示されているように、その動作プログラムを格納するプログラム格納部に電気的消去可能な不揮発性メモリ等を用いていて、その動作プログラムが書換え可能となっているが、このようなICカードでは、動作プログラムの書換えによるICカードの改ざん、そしてその不正使用の危険性がある。

そこで、この発明の目的は、このような従来のICカードにおける動作プログラムが容易に書換えできるという欠点をなくし、以てその改ざんと

か不正使用がされ難い、機密性の高いICカードを提供することにある。

また、この発明他の目的は、ICカードにダウンロードで書込んだ動作プログラムの書換えが権限のあるもの以外できないようなICカードを提供することにあるとする。

この発明のさらに他の目的は、前記のような目的を達成できるICカードの動作プログラム書込み方法を提供することにある。

〔課題を解決するための手段〕

この発明の特徴は、動作プログラムの書込み時にその動作プログラムの識別情報と属性情報を書込み、動作プログラムの書換えを行う場合には、属性情報を参照して、書換え可能な場合のみ書換えを行うようにして、動作プログラムの書換えにおける機密性を向上させたものである。しかも、この場合の属性情報の書換えには、識別情報の組合をもって行い、識別情報の一致による許可制として、特定の限られた者以外は許さないようにしている。

しかし、前記のような目的を達成するためのこの発明のICカードにおける構成は、動作プログラムの書換えが可能か否かを示す書換え可否情報とこの書換え可否情報を書換え可及び書換え不可のいずれかの状態に書換える許可を与えるための照合情報とを記憶するメモリを備えていて、外部からの入力情報と照合情報との一致をもって書換え可否情報の状態を可及び否のいずれか一方の情報に書換え、この書換え可否情報が書換え可となっているときに動作プログラムの書換え処理を実行するものである。

【作用】

このように、ICカードの内部に動作プログラムの書換え可否情報と照合情報とを設けておき、書換え可否情報を参照して動作プログラムの書換え可或いは否（不可）の制御を行い、照合情報の一致により動作プログラムの書換えに関する権限を与えるようにしているので、ICカードの動作プログラム、或いはその書換えに関する機密性が向上し、不正な動作プログラムの書換えを防止す

ることができる。

【実施例】

以下、この発明の一実施例について図面を参照して詳細に説明する。

第1図は、この発明を適用したICカードの一実施例を示すブロック図であり、第2図は、その動作プログラムの書込み処理におけるフローチャート、第3図は、その識別情報及び属性情報の書込み処理におけるフローチャート、第4図は、識別情報及び属性情報の使用状態の一例を示す説明図、第5図は、この発明を適用したICカードの他の実施例を示すブロック図、第6図は、第5図に示すICカードの動作プログラムの書込み処理におけるフローチャート、第7図は、第5図に示すICカードの識別情報及び属性情報の書込み処理におけるフローチャート、第8図は、第5図に示すICカードのプログラム格納部の状態の一例を示す説明図、第9図は、この発明を適用したICカードのさらに他の実施例のブロック図、第10図は、その識別情報及び属性情報の書込み処理

におけるフローチャートである。

ICカード1は、第1図、第5図、そして、第9図に示すように、情報入出力部7と、処理部6、プログラム格納部4、そして情報記憶部5とを備えていて、外部装置8に装着され、この外部装置8（例えば、ICカードリーダー・ライター又はホストコンピュータ）からの信号によって動作を開始する。ICカード1の動作は、処理部6がその内部に有するプログラムにより又はプログラム格納部4にダウンロードで格納されたプログラムを起動することで決定される。また、処理部6は、起動されたプログラムに従って情報入出力部7を介して外部装置8と情報の授受を行うとともに、情報記憶部5或いはプログラム格納部4から情報を読出し、これらに情報を書込む処理を実行する。

ICカード1のプログラム格納部4及び情報記憶部5は、例えば、EEPROM（電気的消去可能な不揮発性メモリ）等の書換え可能な不揮発性メモリで構成されていて、プログラム格納部4には、動作プログラムの属性情報を格納する属性情報格

納部2と動作プログラムの識別情報を格納する識別情報格納部3、そして動作プログラム格納部9とがそれぞれ設けられている。

まず、第1図に示すICカード1の内容から説明すると、属性情報格納部2には、動作プログラムの書換えに関する属性情報（例えば、W（ライト）…書換え可（又は書換え可能、以下同じ）、R（リードのみ）…書換え不可）が記録され、識別情報格納部3には、動作プログラム或いは動作プログラムを書込んだ者の識別情報（例えば、暗証番号、プログラム名等）が記録され、動作プログラム格納部9には動作プログラムが記憶される。

ここで、属性情報は、動作プログラム格納部9に記憶される動作プログラムの書換え可否情報となっていて、識別情報は、属性情報の状態を書換えるための照合情報（書換え許可の条件情報）となっている。これら属性情報と識別情報とは、動作プログラムの書込みと同時に行われても、また、独立に行われてもよい。

したがって、動作プログラムの書込み、書換え

を行う際には、外部装置8からの命令をマイクロプロセッサを有する処理部(CPU)8がデコードし、それが動作プロセッサの書き込みに対するものであるときに、CPU8の内部に記憶された動作プログラム書き込み制御プログラム8aを起動することで行われる。そして、この動作プログラム書き込み制御プログラム8aは、例えば、第2図に示すような処理となる。第2図において、そのステップ101で、まず、属性情報格納部2に属性情報が書き込まれているかを判定し、属性情報が書き込まれていれば、次のステップ102において、その属性情報が書換え可能である否かを判定し、書換え可能である場合には、次のステップ103において、CPU8が動作プログラムの書換えを許可する処理をして、ICカード1は、外部から提供される動作プログラムの書き込み処理を実行する。

このような処理においては、属性情報が書き込まれていることが動作プログラムの書き込み条件となっていて、かつその属性情報が書き込み可の状態に

なっていないければ動作プログラムの書き込みができないことになる。そこで、属性情報を不可の状態にしておくことにより、動作プログラムの書き込みを禁止することが可能である。

このような属性情報自体の書き込みと識別情報の書き込み、そしてこれらの書換えを行うには、CPU8の内部に記憶された管理情報書き込み制御プログラム8bを起動することにより行われる。この管理情報書き込み制御プログラム8bは、例えば、第3図に示すような処理に従って行われる。

第3図において、ステップ111で、まず、識別情報格納部3に識別情報が書き込まれているか否かを判定する。識別情報が未書き込みの場合には、ステップ112aへと移り、CPU8が人力情報のうちの所定の情報をデコードして、識別情報の書き込みか否かの判定をして、ステップ113aで識別情報の書き込みを行う。また、識別情報の書き込みでなければ、このプログラムの処理を終了する。

一方、識別情報が書き込み済みであれば、ステップ112で、書き込み済みの識別情報を識別情報格

納部3から読出して、これと入力された識別情報との識別情報同士を照合を行い、ステップ113でその一致か否かを判定し、一致した場合にのみ、ステップ114へと移り、入力された新たな識別情報又は属性情報を受け入れて、CPU8がいずれかであるかを判定し、属性情報格納部2又は識別情報格納部3のうちの対応する格納部に識別情報又は属性情報を格納してその識別情報或いは属性情報の書換え処理を実行する。なお、ステップ112の識別情報の照合の結果不一致であれば、このプログラムの処理は終了する。

さて、ICカード1を製造し、利用するためには、通常、ICカード製造者がICカードを製造し、それを購入したICカード発行者が所望の形態で利用できるようにICカードに所定のデータとか動作プログラム等を書込み、ICカード利用者に発行して、発行を受けたICカード利用者(所持者)がICカードを使うか、ICカード使用者にさらに発行する。

このような場合、ICカード1への動作プログ

ラム書き込みが必要なのは、一般に、ICカードの製造者とICカード発行者である。ICカードの製造者はICチップを用いてICカード1を製造するが、そのICカード1が正しく動作するか、テストする必要がある。そのため、その動作プログラムの1つとしてテストプログラムをICカード1に書き込む必要がある。このとき、第4図の(a)に示すように、ICカード製造者の識別情報(M-ID)を管理情報書き込み制御プログラム8bに従って、まず、識別情報格納部3に書き込み、次にこの識別情報を用いて属性情報(W-書換え可)を書き込む。その後、テスト用の動作プログラム(テストプログラム)を動作プログラム格納部9に書込んでICカード1のテストを行う。正しく動作すると判定されたICカード1は、同図(b)に示すように、ICカード製造者からICカード発行者Aに渡される。このとき、ICカード製造者の書き込んだ識別情報(M-ID)もICカード1と共にICカード発行者Aに通知される。

そこで、ICカード発行者Aは、ICカード1

動作プログラム格納部9に必要な動作プログラムを占込む(このとき先にICカード製造者が書込んだテストプログラムは自動的に書換えられる)。そして、管理情報書込み制御プログラム8bに従ってICカード製造者から通知された識別情報(M-ID)を用いて識別情報を、例えば、発行者等を示す“I-ID”に書換え、属性情報も“R…書換え不可”に書換える。

このようにすれば、動作プログラムの書換えをしようとしても、第2図に示す動作プログラム書込み制御プログラム8aの処理により動作プログラムの書換え不可の判定がなされるために、動作プログラムの書換えは不可能となる。この動作プログラムの書換えは、第3図に示す管理情報書込み制御プログラム8bの処理により属性情報格納部2に記憶された属性情報“R…書換え不可”を属性情報“W…書換え可”に変更しない限りはできない。そこで、識別情報である“I-ID”を知っているICカード発行者A以外にはそれが不可能になる。

第5図は、複数の動作プログラムが格納できるICカード1であって、その一例としてプログラム格納部4は、2つの動作プログラムが格納できるように第1、第2の動作プログラム格納部9a、9bの2つの領域が設けられるようにプログラム格納部4が分けて管理されている。また、プログラム格納部4には、第1、第2の動作プログラム格納部9a、9bにそれぞれ記憶される第1、第2の動作プログラムに対応してそれぞれの属性情報を格納する第1、第2の属性情報格納部2a、2bと、これらに対応する識別情報を格納する第1、第2の識別情報格納部3a、3bとがそれぞれ設けられている。

第1、第2の属性情報格納部2a、2bには、先の実施例と同様に、それぞれ第1、第2の動作プログラム格納部9a、9bに記憶される第1、第2の動作プログラムに対応してそれぞれの動作プログラムの書換えに関する属性情報(例えば、W(ライト)…書換え可、R(リードのみ)…書換え不可)が記録され、第1、第2の識別情報格

そこで、例えば、ICカード発行者Bが動作プログラムの追加を希望した場合には、ICカード発行者Aが識別情報“I-ID”を用いて属性情報を“W…書換え可”とした上でICカード発行者BにICカード1を渡す。そして、ICカード発行者Bが動作プログラムの追加を行った後、ICカード発行者Aが属性情報を再び“R…書込み不可”にする。このような場合にはICカード発行者Aが動作プログラムの書換えに関する権限を持つことになる。この動作プログラムの書換えの権限をICカード発行者Aが放棄する場合には、ICカード1と共に識別情報(I-ID)をICカード発行者Bに通知することで済む。

識別情報(I-ID)を通知したくない場合は、ICカード発行者Aが識別情報(I-ID)を仮の識別情報に書換えた後、ICカード発行者BへICカード1とともに仮の識別情報を通知するようにすればよい。

次に、第5図～第7図に従って他の実施例について説明する。

第3図a、3図bには、動作プログラム或いは動作プログラムを書込んだ者の識別情報(例えば、暗証番号、プログラム名等)が先の実施例と同様にそれぞれの動作プログラムに対応して記憶される。

次に、第6図に従ってその動作を説明すると、そのステップ121で、まず、CPU6が外部装置8から送出された入力情報のうちの所定の位置に置かれた情報をデコードしてそれが動作プログラムの書込みコマンドであるときに、第1の動作プログラム格納部9aに対する書込みであるかを否かを判定する。

前記の判定の結果、第1の動作プログラム格納部9aに対する書込みであるときにはここでYES条件が成立し、次のステップ122aにおいて、第1の属性情報格納部2aに属性情報が書込まれているかを判定する。このとき属性情報が書込まれていると判定されれば、次のステップ123aにおいて、その属性情報が書換え可能であるかを判定し、書換え可能である場合には、次のステップ124aにおいて、CPU6が動作プログラ

ムの書換えを許可する処理をする。そこで、ICカード1は、第1の動作プログラム格納部9aに動作プログラムの書込み処理を行うことができるようになり、外部装置8から送出手される動作プログラムの書込み処理を行った後に、この処理プログラムによる処理を終了する。

なお、CPU6が動作プログラムの書換えを許可する処理としては、例えば、EEPROMで構成されるプログラム格納部4において、通常は、書込み禁止となっている第1、第2の動作プログラム格納部9a、9bのアドレス空間の管理を書込み可とするような処理である。

さて、先のステップ121の判定において、第1の動作プログラム格納部9aに対する書込みでないと判定されれば、ここでNO条件となり、次のステップ122bにおいて、第2の属性情報格納部2bに属性情報が書込まれているかの判定がなされる。この判定で属性情報が書込まれていれば、次のステップ123bにおいて、その属性情報が書換え可能であるか否かの判定をして、それ

が書換え可能である場合には、次のステップ124bにおいて、CPU6が動作プログラムの書換えを許可する処理をする。その結果、ICカード1は、第2の動作プログラム格納部9bに動作プログラムの書込み処理を行うことができるようになり、外部装置8から送出手される動作プログラムの書込み処理を行った後に、この処理プログラムによる処理を終了する。

なお、ステップ122a若しくは122bで属性情報が書込まれていない場合、或いはステップ123a若しくは123bで属性情報が書換え可能となっていない場合には、動作プログラムの書込み処理は行われずに、この処理プログラムによる処理を終了する。

このようにすれば、単に属性情報を不可の状態にしておくだけで、動作プログラムの書込みを禁止することができる。

このような属性情報自体の書込みと識別情報の書込み、そしてこれらの書換えを行う際には、外部装置8から管理情報(属性情報及び識別情報)

の書込みについてのコマンドを送出することで行う。CPU6がこのコマンドを受けてそれをデコードすると、それが管理情報の書込みに対するものであるときにCPU6は、内部に記憶された管理情報書込み制御プログラム8bを起動する。このことで第7図に示す管理情報の書込み処理が行われる。

第7図において、ステップ131で、まず、CPU6が入力情報のうちの所定の位置に置かれたコマンドをデコードしてそれが管理情報の書込み命令であるときに、第1の動作プログラムについての管理情報の書込みであるか否かを判定する。その結果、第1の動作プログラムについての管理情報の書込みであるときにはここでYES条件が成立する。そして、次のステップ132aにおいて、第1の識別情報格納部3aに識別情報が書込まれているかを判定する。識別情報が未書込みの場合には、次のステップ134aへと移り、CPU6が入力情報のうちの所定の位置に置かれた情報をデコードしてそれが識別情報の書込みである

ときに、ステップ138aで第1の識別情報格納部3aへ識別情報の書込みを行い、その後、この処理プログラムによる処理を終了する。また、識別情報の書込みでない場合にはこの処理プログラムによる処理を終了して、別の処理に移る。

一方、ステップ132aの判定で識別情報が書込み済みと判定されれば、ステップ133aで、書込み済みの識別情報を第1の識別情報格納部3aから読出して、これと外部装置8から送出手された第1の動作プログラムについての識別情報との識別情報同士の照合を行い、その結果を一致/不一致フラグとしてメモリのあらかじめ予定された記憶領域に記憶する。そして、ステップ135aで前記の一致/不一致フラグを参照して、識別情報同士が一致しているか否かを判定し、一致している場合にのみ、ステップ137aへと移り、入力された新たな第1の動作プログラムについての識別情報又は属性情報を受入れて、これらがいずれかの識別情報又は属性情報であるかをCPU6が判定した後に、CPU6は、判定結果に応じて

第1の属性情報格納部2a又は第1の識別情報格納部3aのうちの対応する格納部に識別情報又は属性情報を格納する。このことで、識別情報或いは属性情報の書換え処理が行われる。そして、この後にこの処理プログラムによる処理を終了する。なお、ステップ135aの判定の結果が不一致であれば、そこで、NO条件となり、この処理プログラムによる処理は終了する。

また、先のステップ131の判定において、第1の動作プログラムについての管理情報の書込みでなければ、ここでNO条件となり、ステップ132bへと移行し、ここにおいて、第2の識別情報格納部3bに識別情報が書込まれているかを判定する。この判定で識別情報が未書込みの場合には、次のステップ134bへと移行し、CPU6が入力情報のうちの所定の位置に置かれた情報をデコードしてそれが識別情報の書込みであるときに、ステップ138bで第2の識別情報格納領域3bへ識別情報の書込みを行い、その後、この処理プログラムによる処理を終了する。なお、この場合、

識別情報の書込みでない場合にはこの処理プログラムによる処理を終了して、他の処理となる。

また、ステップ132bの判定で識別情報が書込み済みと判定されれば、ステップ133bで、書込み済みの識別情報を第2の識別情報格納部3bから読出して、これと入力された第2の動作プログラムについての識別情報との識別情報同士の照合を行い、ステップ135bでその一致か否かを判定し、一致した場合にのみ、ステップ137bへと移行し、入力された新たな第2の動作プログラムについての識別情報又は属性情報を受入れて、CPU6がいずれかであるかを判定して第2の属性情報格納部2b又は第2の識別情報格納部3bのうちの対応する格納部に識別情報又は属性情報を格納する。その後、この処理プログラムによる処理を終了する。なお、ステップ135bの識別情報の照合の結果不一致であれば、この処理プログラムによる処理は終了する。そして、他の処理となる。

次に、以上のような動作をするICカードの発

行手順について第8図に従って説明する。

まず、プログラム格納部4に何も書込まれていない第8図(a)に示す状態のICカード1に対し、ICカード製造業者が外部装置8にこれを装着して、第1の動作プログラムに対する識別情報(M-ID)の書込みコマンドを外部装置8からICカード1に送出する。ICカード1のCPU6は、外部装置8から送出されたこのコマンドをデコードし、管理情報の書込みコマンドであることを知り、前記のデコードに応じて管理情報書込み制御プログラム8bを起動する。次に、CPU6が入力情報のうちの所定の位置に置かれた情報をデコードして第1の動作プログラムについての管理情報の書込みであることを知り、第1の識別情報格納部3aに識別情報が書込まれているかどうかを調べる。そして、識別情報が書込まれていないと判定すると、CPU6が入力情報のうちの所定の位置にある情報をデコードして識別情報の書込みであることを知り、第1の識別情報格納部3aに識別情報(M-ID)の書込みを行い、そ

の後、CPU6は、この処理プログラムによる処理を終了するとともに、外部装置8に管理情報書込み制御プログラムによる処理が終了した応答を返す。このことにより、外部装置8は、そのディスプレイ等を介してICカード製造者に管理情報書込み処理が終了したことを知らせる。

なお、以上の処理において、入力情報のうちの所定の位置に置かれた情報をデコードして管理情報の書込みや識別情報の書込みであることを知る処理は、最初に外部装置8から送出された電文において管理情報の書込みコマンドとともに送出された所定の位置にある情報をデコードするものであっても、また、独立にICカード1に何かを処理させるたびごとに、外部装置8から電文を送出する形式を採り、各電文のコマンドの位置にある情報をデコードすることであってもよい。以下の説明においても、また、第1図の実施例においても以上のことは同様に適用される。

さて、以上のような処理により第8図(a)に示すICカード1は、同図(b)に示す状態とな

る。

次に、ICカード製造者が外部装置8を介して第8図(b)に示す状態のICカード1に対して第1の動作プログラムに対する管理情報の書き込みコマンドを送出すると、ICカード1のCPU6が外部装置8から送出されたコマンドをデコードし、管理情報の書き込みコマンドであることを知り、管理情報書き込み制御プログラム6bを起動して、CPU6が入力情報のうちの所定の位置にある情報をデコードして第1の動作プログラムについての管理情報の書き込みであることを知り、第1の識別情報格納部3aに識別情報が書き込まれているかどうかを調べる。ここで、識別情報が書き込まれていると判定されると、CPU6は、第1の識別情報格納部3aから識別情報(M-ID)をICカード1内部で送出するとともに、外部装置8に対して識別情報の入力待ち状態であることの応答を返す。

この応答を受けた外部装置8は、ICカード製造者にICカード1が識別情報の入力待ち状態であ

ることを知らせ、識別情報を入力するようにメッセージする。

そこで、ICカード製造者は、外部装置8を介して第1の動作プログラムに対する識別情報(M-ID)を入力するとともに、第1の動作プログラムに対する属性情報(W)の書き込み指令をする。このような入力を受けた外部装置8は、識別情報と属性情報の書き込みコマンドとを電文としてICカードに送出する。

この電文を受けたICカード1では、CPU6が第1の識別情報格納部3aから送出した識別情報と外部装置8から送出された第1の動作プログラムについての識別情報との照合を行う。そして、CPU6は、これらの一致を確認した後に、入力情報のうちの所定の位置にある情報をデコードして第1の動作プログラムに対する属性情報(W)の書き込みであることを知り、第1の属性情報格納部2aに属性情報(W)の書き込み処理を行う。その後、CPU6は、この処理プログラムによる処理を終了させるとともに、外部装置8に対して管

理情報書き込み制御プログラム6bによる処理が終了した応答を返す。その結果、外部装置8によりICカード製造者は、管理情報書き込み処理が終了したことを知らされる。この処理の結果として、第8図(b)のICカード1は、同図(c)に示す状態となる。

次に、ICカード製造者は、外部装置8を介してICカード1に第1の動作プログラム格納部9aへ動作プログラムの1つとしてICカードの動作をテストするためのテストプログラムを書込むコマンドを送出する。

ICカード1は、そのCPU6で送出されたコマンドをデコードして動作プログラムの書き込みコマンドであることを知り、動作プログラム書き込み制御プログラム6aを起動する。そして、CPU6が入力情報のうちの所定の位置にある情報をデコードして第1の動作プログラム格納部9aに対する書き込みであることを知り、第1の属性情報格納部2aに属性情報が書き込まれているかどうか調べる。ここで、第1の属性情報格納部2aに属性

情報が書き込まれており、その属性情報が(W)であるので、これを判定の結果として得たCPU6は、書き込み可である旨の応答を外部装置8に返して、外部装置8から次に送出されるプログラムのデータの待ち状態に入る。外部装置8は、すでに送出するプログラムが指定されていれば、それを送出するが、そうでなければ、ICカード製造者に対してプログラムを送出する処理をするようにメッセージする。そして、外部装置8からテストプログラムが送出される。

外部装置8から送出されるプログラムのデータを受けると、CPU6は、それを第1の動作プログラム格納部9aに書き込み、動作プログラム(現在はICカード1のテストプログラム)の書き込み処理を実行する。そして、この書き込み終了後にCPU6は、この処理プログラムによる処理を終了するとともに、外部装置8に動作プログラム書き込み制御プログラム6aによる処理が終了した応答を返す。そこで、外部装置8を介してICカード製造者が動作プログラム書き込み処理が終了した

ことを知る。この処理により第8図(c)のICカード1は同図(d)に示す状態となる。

その後、ICカード製造者は、第1の動作プログラム格納部9aに記憶されたテストプログラムを使ってICカード1の動作テストを行い、これが正しく動作することが確認(判定)されたときに、第8図(d)に示す状態のICカード1をICカード発行者Aに渡すとともに、テストプログラムに対する識別情報(M-ID)をICカード発行者Aに通知する。

次に、ICカード発行者Aは、外部装置8を介して照合情報(M-ID)を入力して、第8図(d)に示す状態のICカード1に対して(M-ID)の照合を行って識別情報(M-ID)を独自に設定した識別情報、例えば、(I-ID)に書き換える(第8図(e)のICカード1参照)。そして、第1の動作プログラム格納部9aへの動作プログラム(例えば、動作プログラムP)を前記と同様な処理をして書き込む。

このとき、第8図の(f)に示すように、先に

第1の動作プログラム格納部9aに書込まれているテストプログラムが動作プログラムPに書き換えられる。したがって、テストプログラムがICカード内部に残ることはない。

以上のようにしてICカードの発行が行われるが、ここで、ICカード発行者Aが他人による動作プログラムPの書き換えを不可としたい場合には、CPU8により管理情報書き込み制御プログラム8bを実行させて第1の識別情報格納部3aの識別情報の照合を行って、第1の属性情報格納部2aに、例えば、Rの情報を書き込ませる処理をする。このようにすれば、第1の属性情報格納部2aに記憶された属性情報をWからRに書き換えることができ、以後は、識別情報(I-ID)を使って動作プログラムPに対する属性情報をRからWに書き換えられない限り、動作プログラムPの書き換えができないことになる。これが第8図(g)に示す状態のICカード1であり、このようにすることでICカード1のセキュリティを向上させることができる。

また、ICカード発行者Aのほかに、ICカードを直接使用する人又はその間にこのICカードを利用してICカード使用者に提供するようなICカード利用者Bがいる場合には、ICカード発行者Aは、ICカード利用者Bに対して利用者Bが作成する動作プログラムについてその自由な書き換えを許可し、かつ、その書き換え禁止ができないようにすることができる。

これは、ICカード発行者AがICカード1の第2の動作プログラム格納部9bへICカード利用者Bの作成した動作プログラムQを書込ませることで実現できる。すなわち、ICカード1のCPU8に管理情報書き込み制御プログラム8bを実行させて第2の識別情報格納部3bに識別情報(I-ID)を書込む。この状態を示すのが第8図の(h)のICカード1である。さらに、第2の属性情報格納部2bに属性情報Wを書込む。その状態を示すのが第8図(i)のICカード1であり、このICカードをICカード利用者Bに渡せばよい。

ICカード利用者Bは、第8図(i)の状態のICカード1の第2の動作プログラム格納部9bに動作プログラムQを書込んで第8図(j)の状態のICカードにするが、動作プログラムQに対する属性情報WをRに変えることができないので、動作プログラムQを書き換え不可能にすることはできない。

ここで、ICカード利用者Bが動作プログラムQを書き換え不可能にしたい場合には、第8図(j)のICカード1をICカード発行者Aの所へ持って行き、ICカード利用者Bが指定する動作プログラムQに対する仮の識別情報(C-ID)を第2の識別情報格納部3bに書いてもらって第8図(k)に示すICカード1にすることで簡単にできる。

このようにした後は、ICカード利用者Bが動作プログラムQに対する仮の識別情報(C-ID)を使って管理情報書き込み制御プログラム8bで第2の識別情報格納部3bに記憶された(C-ID)を動作プログラムQに対する識別情報(B-ID)

に書換えるとともに、第2の属性情報格納部2bに記憶されたWをRに書換えて第8図(l)に示す状態のICカード1にする。

一方、ICカード発行者Aが他人によるICカードの第2の動作プログラム格納部9bへの動作プログラム書込みを許さない場合には、第8図(g)に示す状態のICカード1の第2の識別情報格納部3bに(I-ID)を書込んで、第8図(h)に示す状態にする。次に、第2の属性情報格納部2bにRを書込んで第8図(m)に示す状態のICカード1にすれば済む。

また、ICカード発行者AがICカード利用者BによるICカード1の第2の動作プログラム格納部9bへの動作プログラムQの書込み及びその動作プログラムQが書換え不可となることを最初から許す場合には、ICカード1の第2の識別情報格納部3b及び第2の属性情報格納部2bに何も書込んでいない状態のICカード、すなわち、第8図(g)の状態のICカード1をICカード利用者Bに渡せばよい。

内部の識別情報との照合を行う。そして、ステップ143において識別情報が一致しているか否かを判定して、これらが一致しているときに、ステップ144で第1の属性情報格納部2a或いは第2の属性情報格納部2bのいずれかに属性情報の書込みを行って、この処理プログラムの処理を終了する。また、ステップ143の判定で不一致のときにはこの処理プログラムの処理を終了させる。さらに、ステップ141の判定で識別情報が書込み済みでなければ、ステップ142aへと移行して識別情報の書込み処理か否かの判定して、識別情報の書込み処理のときにステップ143aで識別情報の書込みを行い、そうでないときには、この処理プログラムの処理を終了する。

このようにすれば、格納される動作プログラムの数にかかわらず、識別情報の数を低減させることができ、その識別情報の記憶領域を小さくできる。

次に、第9図の実施例におけるICカードの発行について、システムプログラムとアプリケーション

以上の実施例では、ICカード1のプログラム格納部4に2つの動作プログラムが入れられる場合を例としているが、これは、3つ以上の動作プログラムが入れられるようにしてもよく、動作プログラムの数が多ければ、また、それに対応して識別情報或いは属性情報の記憶領域を採れば、それだけ、さらに多くの条件でのICカードを発行することが可能となる。

次に、この発明のさらに他の実施例について第9図、第10図を参照して説明する。

第9図は、第5図に示す第1、第2の識別情報3a、3bの2つの識別情報を共通にして、それを1つの識別情報3として第1、第2の動作プログラム9a、9bに共通に使用するようにした例である。その動作プログラムの書込み処理については、第6図の場合と同様であるので割愛する。

識別情報の照合による属性情報の書込み処理については、第10図に示すように、ステップ141で識別情報書込み済みか否かを判定し、ステップ142で外部装置8から送山された識別情報と

ンプログラムを記憶する例について説明する。なお、識別情報の書込みやその後のテストプログラムの書込みまでの手続き等は、第5図に示す実施例と同様であるので割愛する。

前述したように、ICカード1のテストを行い、正しく動作すると判定されたICカード1がICカード製造者からICカード発行者Aに渡される。このとき、前述したように、ICカード製造者の書込んだ識別情報(M-ID)もICカード1とともにICカード発行者Aに通知される。ICカード発行者Aは、必要な動作プログラムの1つであるシステムプログラムをテストプログラムの上からICカード1の第1の動作プログラム格納部9aに書込み、テストプログラムをこれに書換える。このとき書込まれるシステムプログラムとしては、例えば、ICカード1のハードウェアの制御、アプリケーションプログラムの管理、アプリケーションプログラムからの処理要求のサポート等の機能を持つものである。

次に、管理情報書込み制御プログラム8bに従

ってICカード製造者から通知された識別情報(M-ID)を用いて識別情報を、例えば、発行者等を示す“I-ID”に書換え、第1の属性情報格納部2aの属性情報も“R…書換え不可”に書換える。このようにすれば、システムプログラムの書換えをしようとしても、管理情報書込み制御プログラム6bの処理により動作プログラムの書換え許可処理がなされるためにシステムプログラムの書換えは不可能となり、識別情報である“I-ID”を知っているICカード発行者Aのみがそれを行うことが可能である。

ここで、ICカード利用者Bが、例えば、アプリケーションプログラムの追加を希望した場合には、ICカード発行者Aが第2の属性情報格納部2bの属性情報を“W…書換え可”とした上でICカード利用者BにICカード1を渡すものである。このとき、ICカード利用者Bは、アプリケーションプログラムの追加を行うことができる。

この場合、ICカード利用者Bは、アプリケーションプログラムの書換えは自由にできるが、シ

ステムプログラムを書換えることはできない。また、ICカード発行者Aがシステムプログラムの書換えをしたい場合には、ICカード利用者BからICカード1を回収し、その第1の属性情報格納部2aに記憶された属性情報“R…書換え不可”を属性情報“W…書換え可”に変更することにより行うことができる。

以上説明してきたが、実施例では、属性情報格納部2と識別情報格納部3をプログラム格納部4に設けているが、これは情報記憶部5に設けてもよく、書換え可能なメモリの領域に設けられればどこでもよい。また、属性情報格納部2と識別情報格納部3とは、連続した1つの情報の一部として割り振られていてもよい。この場合には、その格納部は1つであって、ここから読出した情報の一部をそれぞれ利用することになる。さらに、属性情報と識別情報とは、動作プログラムの特定の位置に配置されてもよい。

また、動作プログラム書込み制御プログラム6aとか、管理情報書込み制御プログラム6bは、

CPU8側に内蔵されたROM又はマスクROM等に記憶されていることがベターであるが、これは、必ずしもCPU8側に記憶されている必要はなく、これらをプログラム格納部4に記憶しておいてもよい。また、このプログラム格納部4は、EEPROMである必要はなく、RAMであってもよい。

なお、各実施例における情報入出力部7と処理部8とは、一体となっていて、CPU8がプログラムを実行することでこれらが実現されてもよいことはもちろんである。

【発明の効果】

以上説明したように、この発明にあっては、ICカードの内部に動作プログラムの書換え可否情報と照合情報とを設けておき、書換え可否情報を参照して動作プログラムの書換え可或いは否の制御を行い、照合情報の一致により動作プログラムの書換えに関する権限を与えるようにしているので、ICカードの動作プログラム、或いはその書換えに関する機密性が向上し、不正な動作プロ

ラムの書換えを防止することができる。

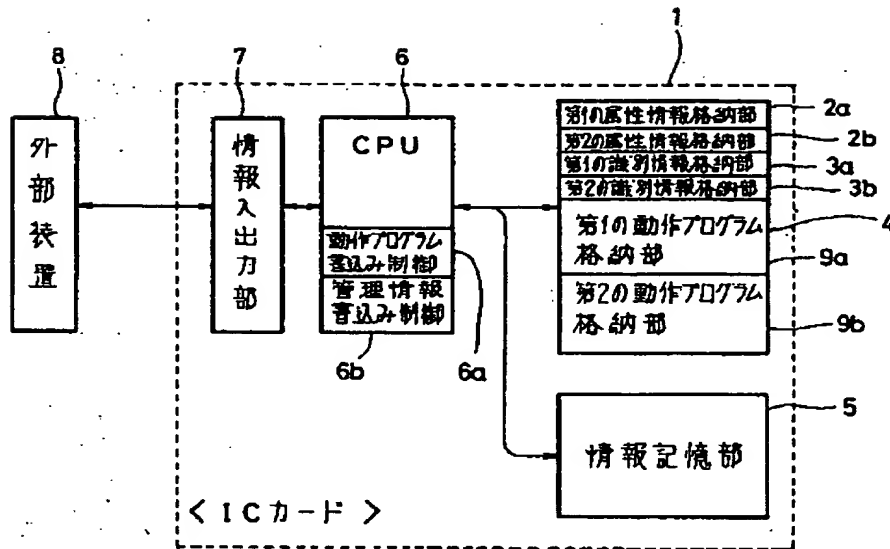
4. 図面の簡単な説明

第1図は、この発明を適用したICカードの1実施例を示すブロック図、第2図は、その動作プログラムの書込み処理におけるフローチャート、第3図は、その識別情報及び属性情報の書込み処理におけるフローチャート、第4図は、識別情報及び属性情報の使用状態の一例を示す説明図、第5図は、この発明を適用したICカードの他の実施例を示すブロック図、第6図は、その動作プログラムの書込み処理におけるフローチャート、第7図は、その識別情報及び属性情報の書込み処理におけるフローチャート、第8図は、第5図の実施例におけるプログラム格納部の使用状態の一例を示す説明図、第9図は、この発明を適用したICカードのさらに他の実施例のブロック図、第10図は、その識別情報及び属性情報の書込み処理におけるフローチャートである。

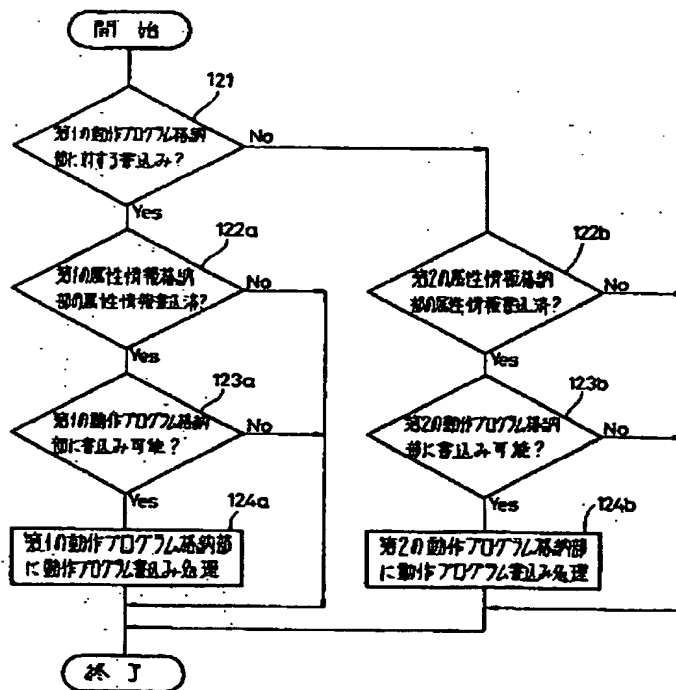
1…ICカード、2…属性情報格納部、

2a…第1の属性情報格納部、2b…第2の属

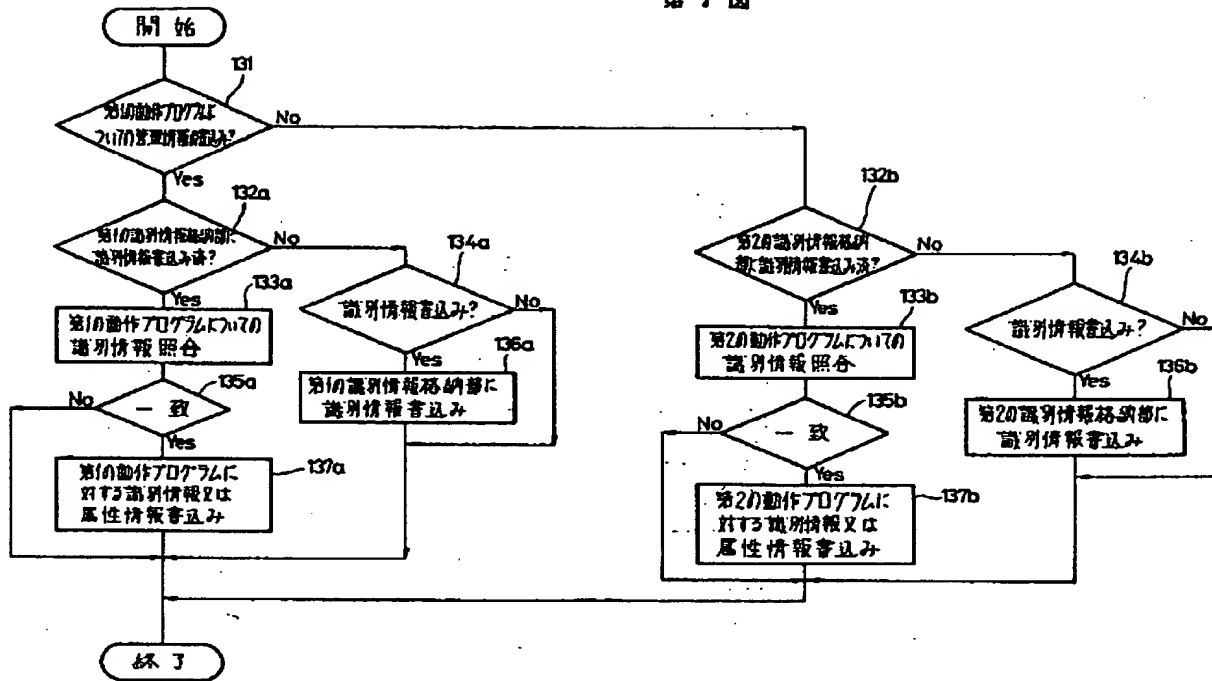
第 5 図



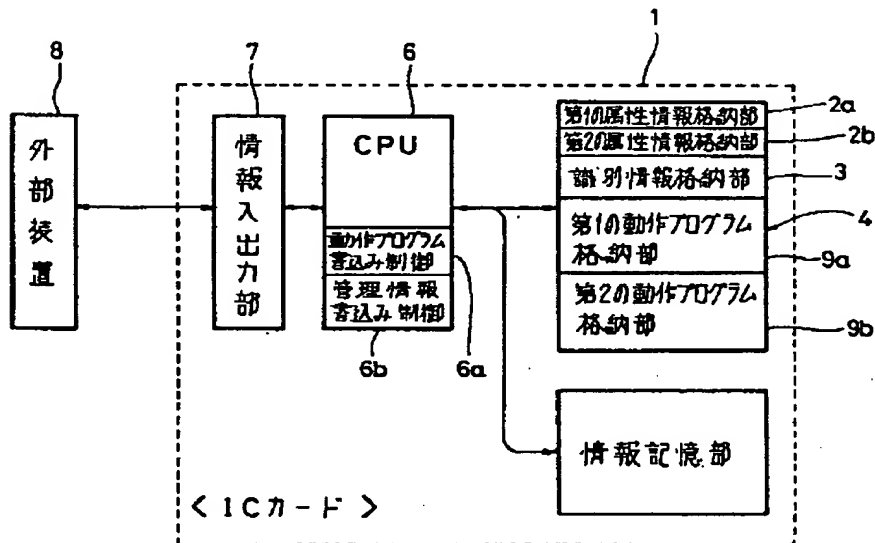
第 6 図



第 7 図



第 9 図



第 10 図

